

## United States District Court

DISTRICT OF DELAWARE

In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

The premises located at

Wilmington, Delaware

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

CASE NUMBER: 08- 129 M

I Theodore J. Theisen being duly sworn depose and say:I am a(n) Special Agent, Federal Bureau of Investigation and have reason to believe  
Official Titlethat ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

., Wilmington, Delaware (as more fully described in Attachment A)

in the District of Delaware

there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence, fruits and instrumentalities of the unlawful transportation, receipt and possession of child pornography (as more fully described in Attachment B)

concerning a violation of Title 18 United States Code, Section(s) 2252 & 2252A.

The facts to support a finding of Probable Cause are as follows:

See Attached Affidavit

Continued on the attached sheet and made a part hereof.

☒ Yes ☐ No

Reviewing AUSA: Edward J. McAndrew

Signature of Affiant  
Theodore J. Theisen, Special Agent  
FBI

Sworn to before me, and subscribed in my presence

Date

July 28th, 2008

at Wilmington, Delaware  
City and StateLeonard P. Stark  
United States Magistrate Judge  
Name and Title of Judicial Officer

Signature of Judicial Officer

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE )  
SEARCH OF: )  
THE PREMISES KNOWN AS )  
Wilmington, Delaware )

Case No.08- 129M

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as , Wilmington, Delaware is identified as follows:

This residence consists of a two story, single family dwelling with a front brick exterior. This house has a brown roof and red shutters. The number "17" is posted above the front door.



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

IN THE MATTER OF THE	)	
SEARCH OF:	)	
THE PREMISES KNOWN AS	)	Case No.08- 129M
	)	
Wilmington, Delaware	)	- - - - -

**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

A. images of child pornography or child erotica and files containing images of such in any form wherever it may be stored or found including, but not limited to:

I. any computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

- B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:
- I. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
  - ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
  - iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
  - iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256;
  - v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;
- C. credit card information including but not limited to bills and payment records, including but not limited to records of internet access;
- D. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;
- E. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access,

and handwritten notes.; and

- F. records or other items that evidence subscription to or use of internet newsgroups or Giganews.com.



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

IN THE MATTER OF THE	)	
SEARCH OF:	)	
THE PREMISES KNOWN AS	)	Case No.08- 129M
	)	
Wilmington, Delaware	)	

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Theodore J. Theisen, a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Wilmington, Delaware Resident Agency, being duly sworn, depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI). I have been employed by the FBI since March of 2004. I have successfully completed the following FBI cyber crime courses: Cyber Investigative Techniques and Resources, Network Security Essentials, Network Investigative Techniques for Agents, Counterterrorism & Counterintelligence Investigations for Cyber Investigators, Advanced Network Investigation Techniques/UNIX, Wireless Computer Intrusion Techniques, Crimes Against Children - Juvenile Issues, Crimes Against Children - Basic, Image Scan, and Linux for Law Enforcement Officers. Prior to working for the FBI, I was employed in the Information Technologies field for approximately six years. During that time, I gained experience in systems engineering, programming, automation and systems management. I have held positions as a Computer Programmer, a Systems Management Engineer, and an Outage Analyst. I am familiar with many

different Operating Systems, including Microsoft Windows and all of its versions and various versions of UNIX and Linux. In addition, I have industry recognized Microsoft Certifications as a Microsoft Certified Professional plus Internet (MCP+I), and a Microsoft Certified Systems Engineer (MCSE).

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I am investigating the activities of Edward Brosky, or any other person, who used a computer connecting to the internet from a service and billing address of ' Wilmington, Delaware ) (the "SUBJECT PREMISES"). As will be shown below, there is probable cause to believe that someone using a computer at the SUBJECT PREMISES has transported, received and possessed child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I am submitting this affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, which is more particularly described in Attachment A, and the seizure of the items more particularly described in Attachment B.

4. All information contained in this affidavit is either personally known to the affiant or has been related to the affiant by other Special Agents of the Federal Bureau of Investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, U.S.C. §§ 2252 and 2252A, are presently located at the SUBJECT PREMISES.

### **STATUTORY AUTHORITY**

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of a minor engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce. 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

### **DEFINITIONS**

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where the production of the visual



depiction involved the use of a minor engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables

and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work.

Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which preform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the

Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l. An Internet Service Provider (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines/cables, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP such as Usenet (newsgroups) and chat/messaging functions. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information,

posting information, account application information, customer service information and other information, both in computer data format and in written record format.

m. A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients."

n. "Usenet" is a service on the Internet which utilizes a network of computers to facilitate the posting of messages, also referred to as articles, in public virtual locations known as "newsgroups." Usenet began as a simple discussion forum for exchanging text messages, but has grown into a hugely distributed file sharing network where software, music, pictures, and videos can be easily traded and shared. These files are posted and retrieved from newsgroups by attaching them to newsgroup messages/articles. Usenet hosts more than 150,000 newsgroups that are organized by topic. To use this service, an individual must use a client application (software), commonly referred to as a news reader, to post and/or read messages to/from a Usenet server. Through the Internet, the server then passes the message on to other servers until it has been replicated or propagated on Usenet servers worldwide. Other individuals can then download the message by accessing their respective Usenet server via their personal (client) computers. To participate in a newsgroup, an individual must either access a Usenet server operated by their ISP, or subscribe to a separate Usenet service, commonly referred to as a News Service Provider (NSP), which is typically a commercial entity or organization that provides Usenet news as its primary or sole activity.

o. Newsgroups follow a particular naming convention which provides the user with an idea of what type of group, or what type of material or discussion a person would

expect to find in that specific newsgroup location. Many Usenet newsgroups have a branch from the root alt. category (i.e. alt.binaries) where hundreds of newsgroups exist that are solely for the purpose of transferring binary files, rather than readable text messages. Newsgroups are categorized by one of approximately eight different Usenet categories:

Alt.\* = alternative material

Misc.\* = misc. topics (e.g. education, items for sale, etc.)

News.\* = discussions about news material

Rec.\* = recreation and entertainment topics

Sci.\* = science related topics

Soc.\* = social issues and topics

Rel.\* = religious related topics

Humanities.\* = fine arts, literature and philosophy

p. An example of the newsgroup "alt.binaries.pictureserotica.pre-teen"

would breakdown as follows:

"alt" ... "alternative" - not yet formally accepted material.

"binaries" ... a file of some kind: image, sound, program, etc. (typically means 'not just text').

"erotica" and "pre-teen" ... more than likely discusses or depicts images of erotic or pre-teen material.

q. There are generally two types of files uploaded to newsgroup locations: text or binary. A text file is just that, it includes readable words (i.e. a message/article). A binary



file is comprised of digits rather than text, and can be a music file, picture/video file, a software program, etc.

r. A newsgroup message is preceded by header lines which contain specific or unique information associated with that particular posting. Through the use of this header information, it is possible to identify an individual that posted the newsgroup message. The header contains at least the following header lines:

"From" - contains the electronic mail address and/or a self created nickname of the person who sent the message;

"Date" - the date and time stamp when the message was originally posted to the network;

"Subject" - a short summary of the content of the message to enable a reader to make a decision based on the subject whether to read the message;

"Message ID" - the message's unique identifier. To ensure the uniqueness of the Message ID, it may not be reused during the lifetime of the message;

"Path" - the network path the message took to reach the current system. When a system forwards the message, it should add its own name to the list of systems in the "Path" line.

### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

7. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce

the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

8. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With digital cameras the images can be transferred directly onto a computer. A computer can connect to another computer through the use of telephone, cable, or wireless connections. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as

Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

14. A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the internet. In general, P2P software allows the user

to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Limewire, one type of P2P software, sets up its searches by keyword. The results of the keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

15. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed of the file(s) he/she wants to download. The file is downloaded directly from the computer hosting the file. The downloaded file is stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

16. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Limewire user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a Limewire user downloading an image file receives the entire image from one computer.

17. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular

computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

18. Third party software is available to identify the IP address of the P2P computer sending the file and to identify if parts of the file came from one or more IP addresses. Such software monitors and logs Internet and local network traffic.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

19. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system



and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

21. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem, router, or any other computer hardware or software found at the SUBJECT PREMISES are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

#### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

22. Affiant has been informed that FBI Supervisory Special Agent (SSA) James T. Clemente has worked in the Behavioral Analysis Unit of the FBI since 1998. SSA Clemente has been a special agent with the FBI since 1987. As a member of the Behavioral Analysis Unit, SSA Clemente consults on child exploitation cases throughout the United States, South America,

and certain European and African countries. Since 1998, he has received three Exceptional Performance Awards from the Department of Justice and a Superior Service Award from the FBI. In addition, he has received numerous letters of commendation from state, federal, and local law enforcement in connection with his work in the Behavioral Analysis Unit.

23. SSA Clemente's training has involved a significant number of specialized courses in the area of child exploitation, including, but not limited to the following: Innocent Images On-Line Sex Crimes Against Children; National Crimes Against Children; On-Line Sex Crimes Against Children; Clinical Forensic Psychology; Behavioral Analysis of Violent Crime; Missing and Exploited Children Seminar; Research Methodologies; MO, Ritual & Signature Advanced Seminar; and Criminology. In addition, he has mentored under, worked with, studied the articles of, and taught with Kenneth V. Lanning, a Supervisory Special Agent, FBI (retired as of October, 2000). SSA Lanning has over the past 27 years authored numerous articles on the topic of sexual victimization of children and behavioral analysis of child molesters. His work forms the basis of the behavioral analysis performed by the FBI in child exploitation cases.

24. SSA Clemente has assisted in the writing of numerous search warrant affidavits and has testified as an expert witness in federal court in the areas of child sex offender behavior, child sexual victimology and child pornography. He has given over 100 presentations and lectures to local, state and federal law enforcement agencies, prosecutors, and health care professionals throughout the United States on various topics related to child exploitation, including, but not limited to the following topics: Behavioral Analysis of Child Sex Crimes Offenders, On-Line Sex Crimes Against Children, and Equivocal Death Investigations.

25. As a member of the Behavioral Analysis Unit, SSA Clemente has analyzed and consulted on between one and two hundred child sexual exploitation and victimization cases a year. His analyses are based on all available evidence, including chat records, image collection analysis, collection themes, possession of erotica, possession of sexual paraphernalia, fantasy literature and writings, other relevant acts, and background information. The vast majority of the cases he has analyzed have involved either Preferential or Situational Sex Offenders. His role in these cases has varied as follows: analyzing investigative results for the purpose of making investigative suggestions, providing expert affidavits for search warrant applications, providing interview strategies for subjects and victims, consulting with local, state and federal prosecutors on trial strategies. In addition, SSA Clemente has interviewed between 80 and 100 offenders himself. A behavioral assessment is not a clinical diagnosis; rather, it is a law enforcement tool used to identify and predict offender behavior.

26. SSA Clemente advises of the following traits and characteristics that are generally found to exist and be true in cases involving individuals who collect child pornography:

- a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
- b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text

that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.

### **BACKGROUND OF THE INVESTIGATION**

27. On April 24, 2008, while conducting an online undercover session, SA Robert J. E. Blackmore, of the Minneapolis Division of the FBI, entered the publicly accessible newsgroup "alt.binaries.camille." While in this newsgroup, SA Blackmore observed that multiple user names had made posts with titles commonly associated with child pornography. He observed that multiple postings were made on April 11, 2008 and April 18, 2008 by a user identifying himself as "Ali-Baba." Postings made by Ali-Baba contained the subject lines:

For Posters & Group All I Have>yEnc "ln-254-15.jpg" (1/1)

For Newman, Posters & Group >yEnc "pret-011a-053.jpg" (1/1)

28. SA Blackmore then downloaded over 100 postings made by Ali-Baba, each of which contained a single image. Many of the images were child pornographic in nature. For example, one of the files that was downloaded on April 11, 2008 was named "ln-254-22.jpg." This file depicts a prepubescent female, appearing to be approximately nine or ten years of age, posing naked with her legs spread exposing her vagina. Another example is a file that was downloaded on April 18, 2008 and named "pret-011a-020.jpg." This image depicts a prepubescent female, appearing to be approximately nine or ten years old, sitting naked on a swing with her legs spread exposing her vagina. Also downloaded on April 18, 2008 was a file with the name "pret-011a-118." This file depicts an unclothed prepubescent female who appears



to be approximately nine or ten years of age with one of her legs bound with a green rope elevated above her head exposing her vagina and anus.

29. Header information in these posts indicated that they were posted through the news provider Giganews.com.

30. On April 28, 2008, SA Blackmore served an Administrative Subpoena on Giganews.com requesting subscriber information for the account used by Ali-Baba to post the header information associated with the child pornographic images that SA Blackmore had downloaded from the newsgroup. In response, Giganews.com advised that the above headers were posted by the account subscribed to by: Edward Brosky, [REDACTED], Wilmington, DE. Giganews.com also provided the type and number of the credit card that Brosky used when subscribing to this service.

31. Pursuant to the Administrative Subpoena, Giganews.com also provided log files indicating that Edward Brosky's account used the IP address 68.238.233.31 from 14:34 Central Standard Time (CST) on March 16, 2008 through 07:56 CST on April 18, 2008. The account used IP address 71.126.122.200 from 12:32 CST on April 18, 2008 through 15:02 CST on April 30, 2008.

32. Using a publicly available software tool, SA Blackmore conducted a whois lookup of the IP addresses 68.238.233.31 and 71.126.122.200, which showed that they resolved to the internet service provider Verizon Internet Services.

33. On May 6, 2008, an Administrative Subpoena was served upon Verizon for subscriber information for the account(s) that were using IP addresses 68.238.233.31 and 71.126.122.200 at the dates/times the images of child pornography were posted by Ali-Baba.

34. On May, 10, 2008, Verizon Internet Services advised SA Blackmore that for all of the requested dates/times, the above IP addresses were assigned to an internet service account subscribed to by: Edward Brosky, [REDACTED] Wilmington, Delaware [REDACTED]

35. On or about July 8, 2008, a law enforcement officer conducted visual surveillance of the SUBJECT PREMISES, which is pictured in Attachment A and which may be described as a two-story, single family dwelling with a front brick exterior. This house has a brown roof and red shutters. The number "17" is posted above the front door.

36. On or about July 9, 2008, your affiant determined that the Delaware Justice Information System (DELJIS) indicated that Edward A. Brosky's Delaware driver's license, [REDACTED], lists his current address as [REDACTED], Wilmington, DE [REDACTED] which is the same address as the SUBJECT PREMISES.

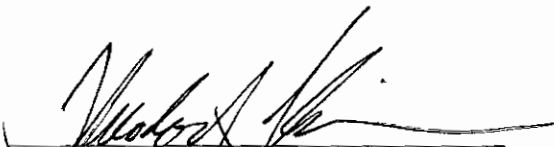
37. On or about July 17, 2008, Delmarva Power confirmed that Edward Brosky has an active account for electric service at the SUBJECT PREMISES.

### **CONCLUSION**

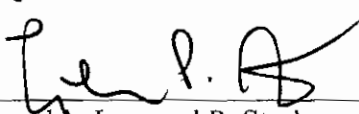
38. Based on the above information, there is probable cause to believe that the SUBJECT PREMISES contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.

39. In consideration of the foregoing, your Affiant respectfully requests that this Court issue a warrant to search the SUBJECT PREMISES, as more particularly described in Attachment A, and to seize the items specified in Attachment B.

Respectfully submitted,

  
SA Theodore J. Theisen, FBI

Sworn and subscribed before me  
this ~~2nd~~ day of July 2008

  
Honorable Leonard P. Stark  
United States Magistrate Judge

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

IN THE MATTER OF THE                     )  
SEARCH OF:                                 )  
THE PREMISES KNOWN AS                 )     Case No.08- 129-m  
  )  
Wilmington, Delaware 1                 )

**ATTACHMENT A**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

The location known as 17 Bellemeade Pl, Wilmington, Delaware 9810 is identified as follows:

This residence consists of a two story, single family dwelling with a front brick exterior. This house has a brown roof and red shutters. The number "17" is posted above the front door.



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

IN THE MATTER OF THE	)	
SEARCH OF:	)	
THE PREMISES KNOWN AS	)	Case No.08- 129M
	)	
Wilmington, Delaware	)	

**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

- A. images of child pornography or child erotica and files containing images of such in any form wherever it may be stored or found including, but not limited to:
- I. any computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;
  - ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
  - iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
  - iv Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;



- B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:
- I. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
  - ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
  - iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
  - iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256;
  - v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;
- C. credit card information including but not limited to bills and payment records, including but not limited to records of internet access;
- D. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;
- E. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access,

and handwritten notes.; and

- F. records or other items that evidence subscription to or use of internet newsgroups or Giganews.com.